Comment. Math.
Univ. St. Pauli
XXVI—1, 1977

Note on projections in 2×2 matrix rings over finite fields

by

Genjiro TANAKA

(Received February 21, 1977)

1. Throughout this note the number p always means a prime one and $p\neq 2$. We let $M_k(R)$ denote the $k\times k$ matrix ring over a ring R. The matrix $X\in M_k(R)$ with the property that $XX^t=X$ is called a projection, where X^t is a transpose of X. The set of all projections in $M_k(R)$ is denoted by $P(k, R)$. Now, let $q=p^n$. In this note $M_k(GF(q))$, $P(k, GF(q))$ are denoted by $M_k(q)$, $P(k, q)$ respectively. If R is a ring with identity, $M_k(R)$ has the $k+2$ trivial projections 0, I (the identity matrix), and I_{ii} ($i=1, 2, \cdots, k$, the matrix units). Notice that if X is a projection, then $X^t=X$. In this section we consider the number of projections in $M_2(R)$, where $R=\bigoplus\sum_{i=1}^{t} GF(q_i)$.

Let $F_q=GF(q)$, $q=p^n$. F_q^* denotes the set of all units of F_q. For F_q we define the following sets;

$$Q_q=\{a^2 \mid a\in F_q^*\},$$
$$S_q=\{b \mid b\in Q_q \text{ and } 1+b\in Q_q\},$$
$$T_q=\{c \mid c\in Q_q \text{ and } 1-c\in Q_q\}.$$

Let $X=[x_{ij}]$ be a projection in $M_2(q)$. If $x_{12}=0$, then $x_{21}=0$ and $X\in\{0, I, I_{11}, I_{22}\}$. If $x_{12}\neq 0$, then $x_{21}\neq 0$ and $x_{22}=1-x_{11}$ from $XX^t=X$. Also we have an equality $x_{11}^2+x_{12}^2=x_{11}$, so we consider the following equation in F_q;

$$x^2-x+b^2=0,\ b\neq 0.$$

Since the characteristic of F_q is not 2, the above equation is equivalent to the next equation in F_q;

$$(2x-1)^2=1-(2b)^2,\ b\neq 0.$$

Thus if $1-(2b)^2\in Q_q\cup\{0\}$, then the above equation has the solutions $x=(1\pm\sqrt{1-(2b)^2})/2$ in F_q. Notice that if $b=\pm 2^{-1}$, then the equation has only one solution $x=2^{-1}$.

The following lemma is the theorem in the section 67 of [1].

LEMMA 1.

$$|S_q|=\begin{cases}(q-3)/4, & \textit{if } -1 \textit{ is a nonsquare in } F_q,\\ (q-5)/4, & \textit{if } -1 \textit{ is a square in } F_q.\end{cases}$$

LEMMA 2. $|T_q|=|S_q|$.

Proof. If $a\in S_q$, then there exists unique $b\in Q_q$ such that $1+a=b$. Since b^{-1}, $b^{-1}a\in Q_q$ and $1-b^{-1}a=b^{-1}$, we have $b^{-1}a\in T_q$. Let $a_i\in S_q$, $b_i\in Q_q$ and $1+a_i=b_i$ $(i=1, 2)$. If $b_1^{-1}a_1=b_2^{-1}a_2$, then $b_2b_1^{-1}a_1=a_2$. Thus

$$a_2=(1+a_2)b_1^{-1}a_1\ ,$$

$$b_1^{-1}a_1a_2^{-1}=1-b_1^{-1}a_1\ .$$

On the other hand we find $1-b_1^{-1}a_1=b_1^{-1}$ from $1+a_1=b_1$. Thus $a_1=a_2$ and $|S_q|\leqq|T_q|$. Similarly we obtain $|T_q|\leqq|S_q|$, and Lemma 2 is proved.

LEMMA 3.

$$|P(2, q)|=\begin{cases}q+3, & \textit{if } -1 \textit{ is a nonsquare in } F_q\ .\\ q+1, & \textit{if } -1 \textit{ is a square in } F_q\ .\end{cases}$$

Proof. There exists the four trivial projections 0, I, I_{11}, and I_{22} in $M_2(q)$. Let $x_{12}=x_{21}=\pm 2^{-1}$, $x_{11}=2^{-1}$ and $x_{22}=1-2^{-1}$, then $X=[x_{ij}]$ are projections in $M_2(q)$.

We now consider the projection $X=[x_{ij}]$ with $x_{12}\neq 0, \pm 2^{-1}$. The number of elements $b\in F_q^*$ such that $1-(2b)^2\in Q_q$ is $2|T_q|$. For each b there exists two $x=(1\pm\sqrt{1-(2b)^2})/2$ in F_q. Thus in $M_q(q)$ there exists $4|T_q|$ projections $X=[x_{ij}]$ with $x_{12}\neq 0, \pm 2^{-1}$. Hence $|P(2, q)|=4|T_q|+2+4$, and Lemma 3 is proved.

Let $R=\bigoplus\sum_{i=1}^t R_i$ be a direct sum of rings. Then $M_k(R)\cong\bigoplus\sum_{i=1}^t M_k(R_i)$. Thus from Lemma 3 we have the following proposition.

PROPOSITION 1. *Let $R=\bigoplus\sum_{i=1}^t F_i$ be the direct sum of finite fields $F_i=GF(q_i)$, $q_i=p_i^n$. If -1 is a nonsquare in F_u $(u=1, \cdots, r)$ and -1 is a square in F_v $(v=r+1, \cdots, t)$, then*

$$|P(2, R)|=\{\prod_{u=1}^{r}(|F_u|+3)\}\cdot\{\prod_{v=r+1}^{t}(|F_v|+1)\}\ .$$

Remark 1. For each $a\in GF(2^n)$, since the characteristic of $GF(2^n)$ is 2, there exists unique $b\in GF(2^n)$ such that $a^2+a=b^2$. Thus it is easily seen that $|P(2, 2^n)|=2^n+2$. Therefore we can derive the formula for $|P(2, R)|$, where R is a direct sum of arbitrary finite fields.

For arbitrary integers $m_1, \cdots, m_t$ such that $(m_i, m_j)=1$ for any pair $i\neq j$, we have $Z/m_1\cdots m_tZ\cong Z/m_1Z\bigoplus\cdots\bigoplus Z/m_tZ$. Since $M_2(2)$ has only four projections, we have the following corollary.

COROLLARY 1. *Let m be an odd integer such that $m\not\equiv 0 \pmod{p^2}$ for any prime p and let $m=p_1\cdots p_rq_1\cdots q_t$ be a prime factorization of m such that $p_i\equiv 3 \pmod 4$ and $q_j\equiv 1 \pmod 4$. Then*

$$|P(2, Z/mZ)|=\left\{\prod_{i=1}^{r}(p_i+3)\right\}\cdot\left\{\prod_{j=1}^{t}(q_j+1)\right\}\ .$$

$$|P(2, Z/2mZ)|=4\left\{\prod_{i=1}^{r}(p_i+3)\right\}\cdot\left\{\prod_{j=1}^{t}(q_j+1)\right\}\ .$$

2. Throughout this section $F_q=GF(q)$, $q=p^n$, is a finite field such that -1 is a nonsquare in F_q.

Let $O(2, q)=\{Y \mid Y^t=Y^{-1}, Y\in GL(2, q)\}$, the orthogonal group, and let $P^*(2, q)=P(2, q)-\{0, I\}$. Each $Y\in GL(2, q)$ induces an automorphism $\hat{Y}$ of $M_2(q)$, where $\hat{Y}: X\to Y^{-1}XY$ for all $X\in M_2(q)$. The kernel of the homomorphism $Y\to\hat{Y}$ is clearly $Sc=\{\lambda I \mid \lambda\in F_q^*\}$, the set of scalar matrices. Thus $PGL(2, q)\subseteqq \mathrm{Aut}(M_2(q))$. In fact it is known that $\mathrm{Aut}(M_n(K))$, where K is a field, is isomorphic to the semi-direct product of $PGL(n, K)$ and $\mathrm{Aut}(K)$[[2], viii 25].

Let $PG(1, q)$ be the projective line of $q+1$ points coordinatized by the elements of F_q and the symbol $\infty=(0, 1)$. $PGL(2, q)$ on $M_2(q)$ is clearly different from $PGL(2, q)$ on $PG(1, q)$ as permutation gaoup.

Let $Y\in O(2, q)$ and $X\in P(2, q)$, then $(Y^{-1}XY)(Y^{-1}XY)^t=Y^{-1}XY$. Thus the set $P^*(2, q)$ is fixed by $O(2, q)$. It is easy to see that $\{\pm I\}$ is the kernel of the action of $O(2, q)$ on $P^*(2, q)$. Therefore the group $O(2, q)/\{\pm I\}$ of order $q+1$ has a faithful permutation representation on $P^*(2, q)$. The degree of the permutation group $O(2, q)/\{\pm I\}$ on $P^*(2, q)$ is $q+1$ by Lemma 3. $O(2, q)/\{\pm I\}$ on $P^*(2, q)$ is isomorphic to $O(2, q)Sc/Sc$ on $PG(1, q)$ as group. We consider the relationship of these permutation groups. We put

$$W=\left\{(\alpha, \beta) \,\middle|\, \begin{bmatrix} \alpha & \beta \\ \beta & 1-\alpha \end{bmatrix} \in P^*(2, q)-\{I_{22}\} \right\}.$$

Notice that if $(\alpha, \beta)\in W$, then $\alpha\neq 0$ and $\alpha^2-\alpha+\beta^2=0$.

LEMMA 4. *Let* $F'=\{\alpha^{-1}\beta \mid (\alpha, \beta)\in W\}$. Then $F'=F_q$ *and for each* $a\in F_q$ *there exists unique* $(\alpha, \beta)\in W$ *such that* $\alpha^{-1}\beta=a$.

Proof. $|W|=|P^*(2, q)-\{I_{22}\}|=q$ by Lemma 3. If $\alpha^{-1}\beta=\gamma^{-1}\delta$ for $(\alpha, \beta), (\gamma, \delta)\in W$, then from $1-\alpha^{-1}+(\alpha^{-1}\beta)^2=0$ and $1-\gamma^{-1}+(\gamma^{-1}\delta)^2=0$ we have $\alpha=\gamma$ and $\beta=\delta$. Thus the mapping $\varphi: (\alpha, \beta)\to\alpha^{-1}\beta$ is one-to-one.

LEMMA 5. *Let* $(\alpha, \beta)\in W$. *Then for arbitrary pair* $u, v\in F_q$, *where* $(u, v)\neq(0, 0)$, *the following* (i), (ii), (iii) *hold*:

(i) *If* $u\alpha+v\beta\neq 0$, *then* $(u\alpha+v\beta)^{-1}\cdot\{u\beta+v(1-\alpha)\}=\alpha^{-1}\beta$.

(ii) *If* $u\alpha+v\beta\neq 0$, *then* $(u\alpha+v\beta)u+\{u\beta+v(1-\alpha)\}v\neq 0$.

(iii) *If* $u\alpha+v\beta=0$, *then* $u\beta+v(1-\alpha)=0$.

Proof. (i). Since $\alpha^2-\alpha+\beta^2=0$,

$$v(\alpha-\alpha^2-\beta^2)=0.$$

Then $$\alpha v(1-\alpha)=v\beta^2.$$

Hence $$\alpha\beta u+\alpha v(1-\alpha)=\alpha\beta u+v\beta^2.$$

(ii). Let $s=(\alpha u+\beta v)u+\{\beta u+v(1-\alpha)\}v$. If $s=0$, then $(\alpha u+\beta v)^{-1}s=u+\alpha^{-1}\beta v=0$ by (i). Thus $\alpha u+\beta v=0$, a contradiction.

(iii). If $\alpha u+\beta v=0$, then $u=-\alpha^{-1}\beta v$. Since $\alpha^2-\alpha+\beta^2=0$, we have

$\beta u+v(1-\alpha)=(-\alpha^{-1}\beta^2+\alpha^{-1}\beta^2)v=0$.

PROPOSITION 2. *If -1 is a nonsquare in $GF(q)$, then $0(2, q)/\{\pm I\}$ on $P^*(2, q)$ is isomorphic to $0(2, q)Sc/Sc$ on $PG(1, q)$ as permutation group.*

Proof. Define the mapping φ: $P^*(2, q)\to PG(1, q)$ by

$$\varphi\colon [x_{ij}]\to[x_{ij}]\varphi=\begin{cases}(0, 1), & \text{if } [x_{ij}]=I_{22}\ .\\ (1, x_{11}^{-1}x_{12}), & \text{if } x_{11}\neq 0\ .\end{cases}$$

By Lemma 4 φ is a one-to-one mapping. We will show that $(Y^{-1}XY)\varphi=(X)\varphi Y$ for all $X\in P^*(2, q)$ and $Y\in 0(2, q)$. Notice that if $Y\in 0(2, q)$, then Y is a following matrix;

$$Y=\begin{bmatrix}u & -v\\ v & u\end{bmatrix}\text{or}\begin{bmatrix}u & v\\ v & -u\end{bmatrix},\quad u^2+v^2=1\ .$$

Suppose that $Y=\begin{bmatrix}u & -v\\ v & u\end{bmatrix}$, $u^2+v^2=1$. If $X=I_{22}$, then $(X)\varphi=(0, 1)$. Thus

$$(X)\varphi Y=(v, u)=\begin{cases}(0, 1), & \text{if } v=0\ ,\\ (1, v^{-1}u), & \text{if } v\neq 0\ .\end{cases}$$

On the other hand,

$$(Y^{-1}XY)\varphi=\begin{bmatrix}v^2 & vu\\ vu & u^2\end{bmatrix}\varphi=\begin{cases}(I_{22})\varphi=(0, 1), & \text{if } v=0\ ,\\ (1, v^{-1}u)\ , & \text{if } v\neq 0\ .\end{cases}$$

Thus $(Y^{-1}I_{22}Y)\varphi=(I_{22})\varphi Y$. If $X=\begin{bmatrix}\alpha & \beta\\ \beta & 1-\alpha\end{bmatrix}$, $\alpha\neq 0$. Then $(X)\varphi=(1, \alpha^{-1}\beta)$ and

$$(X)\varphi Y=\begin{cases}(0, 1), & \text{if } u+\alpha^{-1}\beta v=0\ ,\\ (1, (u+\alpha^{-1}\beta v)^{-1}\cdot(-v+\alpha^{-1}\beta u)), & \text{if } u+\alpha^{-1}\beta v\neq 0\ .\end{cases}$$

On the other hand $Y^{-1}XY=\begin{bmatrix}s & t\\ * & *\end{bmatrix}$,

where

$$s=(\alpha u+\beta v)u+\{\beta u+v(1-\alpha)\}v\ ,$$
$$t=(\alpha u+\beta v)(-v)+\{\beta u+v(1-\alpha)\}u\ .$$

If $\alpha u+\beta v=0$, then $\beta u+v(1-\alpha)=0$ by Lemma 5 (iii). Thus if $u+\alpha^{-1}\beta v=0$, then $Y^{-1}XY=I_{22}$ and $(Y^{-1}XY)\varphi=(0, 1)$. If $\alpha u+\beta v\neq 0$, then $s\neq 0$ by Lemma 5 (ii) and we have $(Y^{-1}XY)\varphi=(1, s^{-1}t)$. Since $s^{-1}t=(u+\alpha^{-1}\beta v)^{-1}\cdot(-v+\alpha^{-1}\beta u)$ by Lemma 5 (i), we find $(Y^{-1}XY)\varphi=(X)\varphi Y$.

By the same manner we obtain $(Y^{-1}XY)\varphi=(X)\varphi Y$ for all $X\in P^*(2, q)$

and $Y=\begin{bmatrix} u & v \\ v & -u \end{bmatrix}$, $u^2+v^2=1$.

Remark 2. Let $O_+(2, q)=\{Y \mid \det Y=1,\ Y \in O(2, q)\}$. The group $O_+(2, q)/\{\pm I\}$ of order $(q+1)/2$ is a subgroup of $PSL(2, q)$. By the same proof of Proposition 2, it is shown that $O_+(2, q)/\{\pm I\}$ on $P^*(2, q)$ is isomorphic to $O_+(2, q)/\{\pm I\}$ on $PG(1, q)$ as permutation group.

References

[1] DICKSON, L. E.; *Linear groups with an exposition of the Galois field theory.* 1901, Dover, New York, 1958.

[2] MCDONALD, B. R.; *Finite rings with identity.* Dekker, New York, 1974.